MASS. SS1.2:F49

ELECTRONIC RECORDS WORKING GROUP

UMASS/AMHERST
312066 0278 1037 0

MASSACHUSETTS CITY CLERKS ASSOCIATION

FINAL REPORT

GOVERNMENT DOCUMENTS COLLECTION
JAN 2 [illegible]
University of Massachusetts
Depository Copy

1995

MASSACHUSETTS TOWN CLERKS ASSOCIATION

William Francis Galvin
Secretary of the Commonwealth

Digitized by the Internet Archive
in 2014

https://archive.org/details/finalreport00elec

Perhaps the most spectacular example of a government agency losing its electronic memory recently occurred at the National Aeronautics and Space Administration when space scientists were eager to access some 1.2 million magnetic tapes of observations that NASA created during three decades of space flight. The researchers were hoping to reveal "long-term trends like global climate change, tropical deforestation, and the thinning of the atmospheric ozone layer," according to NASA....But the information could not be read or sometimes even found. Tapes were uncataloged. Some had been damaged by heat or floods. Many were unlabeled as to which mission or spacecraft or computer system created them. Because no proper archival controls for these records were in place, NASA officials estimate that it will take millions of dollars and years of detective work to link each of the files to their spacecraft or mission and then decode the information so that it can be read by hardware and software now in use.

-- Terry Cook , "It's Ten O'clock: Do You Know Where Your Data Are?", *Technology Review*, January 1995

...[M]any electronic records remain dependent on specific software or hardware....The case of the 1960 U.S. Census is illustrative. The type and format of computer tapes used for census returns in the 1960's became obsolete a few years later. There are only two machines in the world that can read the original data tapes from that census. One machine is in the Smithsonian Institution and the other is in Japan....The incident shows how quickly computer records can become obsolete. If a computer record cannot be read, then for all practical purposes, the record no longer exists.

-- Committee on Government Operations, House of Representatives, Report 101-978, "Taking a Byte Out of History: the Archival Preservation of Federal Computer Records," November 6, 1990

A mid-west manufacturer installed new records management imaging systems for legal documents. Three million dollars of state-of-the-art technology has been installed for 18 months. There are no users yet. The paralegals and lawyers were not consulted on the design nor educated on the system until afterwards. Unfortunately, the indexing design does not work....The index can be modified. That conversion is estimated to take 2,000 days.

-- Thomas H. Johnson and Thornton A. May, *Managing Strategic Imaging Initiatives*, Nolan Norton Institute, December 1990

Information deleted from a computer's memory may not actually disappear, but may simply be dormant, retrievable by an expert and waiting to trap the incautious. A woman suing her former employer for unlawful termination hired evidence specialist John Jessen to assist with her case. In spite of the company's assertion that the employee had been fired for financial reasons only, Jessen was able to recover a deleted e-mail message from the company president ordering the director of human resources to "Get rid of that tight-assed bitch." The company settled out of court for $250,000.

-- Ellen Wright, "Incriminating Data," *Hemispheres*, Pace Communications, Inc., Greensboro, NC

Table of Contents

Executive Summary.....1

Purpose/1

Methodology/1

Summary of issues and recommendations/1

General recommendations/4

Implementation/5

Issues.....6

Preservation/6

Compatibility/9

Legality/12

Access/15

Appendices

A: Working Group Members and Guests

B: List of Recommendations

C: List of Readings

Executive Summary

Purpose
The Electronic Records Working Group (ERWG) was formed by the Office of the Secretary of the Commonwealth, the Massachusetts City Clerks Association, and the Massachusetts Town Clerks Association. The purpose of the group is to identify electronic records concerns and point to potential approaches. The following report describes these concerns and recommends activities to be undertaken by the clerks' associations and the Office of the Secretary to develop solutions and strategies to address problem areas.

Methodology
The working group is nonhierarchical and composed of city and town clerks nominated by their respective statewide associations, representatives of the Massachusetts Archives, Division of Public Records, and the Massachusetts Government Information Systems Association (MGISA). Each of these components brought to the discussions its own sets of concerns and expertise.

At its first meeting, the group identified four electronic records issues of particular concern to municipal clerks: preservation, legality, compatibility, and access. These were explored and concerns prioritized. At subsequent meetings, each issue area was discussed and possible strategies considered. The group studied pertinent articles and unpublished papers, and utilized large and small group discussion. Subject area specialists were invited to facilitate discussion and provide information to group members. After each large group meeting, a subgroup met to review findings, conduct additional research, and develop a discussion paper on the topic addressed at that meeting. This report is based on the large group discussions and subgroup papers; these papers are available upon request.

Summary of issues and recommendations
The areas identified as especially relevant to clerks-- preservation, compatibility, legality, and access-- are not mutually exclusive or exhaustive, but served to organize the work of the group.

Preservation: Many of the records of the clerks' offices have long term value and continue to be referenced ten, fifty, even a hundred years after their creation; in contrast, MGISA reports that, on average, municipalities replace their electronic records systems at less than four year intervals. To confidently commit themselves to information technology, clerks must devise methods and practices that permit them to preserve and secure electronic records beyond the life of the electronic records systems on which the records were created.

Recommendations:

1. Identify and publicize applicable hardware and software standards and operational practices that support forward migration of data to new platforms and software.

2. Develop a set of questions and requirements clerks can use in negotiating and contracting with vendors that will lead to the creation of non-proprietary, reliable, standards-based systems and records.

3. Establish a clearinghouse where clerks can report the success or failure of hardware, software, and media.

4. Review retention schedules to revise retention periods and identify the custodial office and media of the record copy.

5. Formulate uniform migration and preservation policies and procedures that support the preservation of all active and inactive records of long-term value, including security, backup, documentation, testing and migration methods and scheduling.

6. To support disaster recovery efforts, coordinate and share information about the technology environment in each municipality with the goal of assisting municipalities to identify emergency data processing locations.

7. Formulate guidance on risk management analysis to assist clerks in assessing the level of security needed for various systems and records.

Compatibility: Because compatibility influences the ability of records to be converted to new systems, it is closely related to preservation. However, compatibility is also a productivity issue: lack of compatibility can hinder communication and data sharing within and among town offices, municipalities, and local and state government agencies.

***Recommendations*:**

8. Offer an open session at association meetings to allow networking and discussion among municipal clerks regarding software application solutions to the problem of incompatibility within clerks' offices.

9. To promote compatibility, develop standards for functionality of software in an open systems environment.

10. Advocate for municipality-wide, coordinated information technology acquisitions.

11. Promote the the development of compatible records systems within local governments.

12. Explore the advisability of recommending that all on-line interaction between the municipalities and state agencies be conducted via the Voter Registration Information System (VRIS) network.

13. Form a joint association committee to coordinate efforts to share electronic data between the state agencies and the office of the municipal clerk.

Legality: In the past, clerks have used electronic systems to increase access to records in paper format; in these tracking and indexing systems, accuracy rather than legality is the critical concern. As the law and technology develop to allow the use of electronic recordkeeping systems, where records are maintained in electronic format, legality-- the ability to produce a trustworthy record that can withstand impeachment-- will become the paramount issue.

Recommendations:

14. Identify statutes presenting obstacles to the acceptance of electronic recordkeeping systems and draft statutory language that will ensure the legality of a record based upon the circumstances of its creation and maintenance, regardless of the recording medium.

15. Clarify the terms *original* and *copy* as they relate to electronic records.

16. Formulate guidance on the attestation and certification of electronic records.

17. Formulate a uniform set of recordkeeping policies and good practices that can be widely adopted and promoted.

18. Establish clearly defined standards for the creation and maintenance of records that are trustworthy, reliable and legal.

19. Investigate the viability of models for achieving recordkeeping standards, either through a central registry system or by having a single entity set performance standards or regulations for recordkeeping systems.

20. Set standards for the storage, duplication, back up or dispersal of records, and for their proper identification.

21. Establish standards for the use of audit trails to ensure the intellectual security of records.

22. Determine expected longevity of various media and establish guidelines for the periodic recopying of records.

23. Establish standards and time frames for migrating records forward to new operating systems and platforms.

24. Investigate the desirability of alternative storage media for records with long-term value, such as microfilm.

Access: Despite the fact that the public records laws were established before the development of computers, the law has been interpreted on a case by case basis to satisfy most users and requesters of electronic government records. New types of systems, networks, and uses for electronic records present additional challenges to the appropriate provision of access and require further analysis.

***Recommendations*:**

25. Develop uniform guidance on access to electronic records, considering specifically:
    - direct public access to on-line data;
    - methods to protect on-line data from unauthorized public access and alteration;
    - the impact of direct public access to on-line data on the efficiency of government operations;
    - subscription and licensing arrangements for on-line data;
    - the records custodian's responsibility to provide for segregation in systems design; and
    - the public records status of licensed software packages.

26. Investigate the application of the public records law to commercial requests for access to and copies of electronic records.

27. Develop uniform guidance on fees for copies of electronic records.

28. Clarify the term *records custodian* as it applies to electronic records that may exist in more than one location; and the responsibilities of the custodian for access, copying, certification, and preservation.

29. In the context of electronic records systems' ability to manipulate and link data, review data collection requirements and privacy restrictions.

30. Develop uniform guidance for specifying and analyzing index generators included in application software.

31. Establish standard indexing and filing rules for use by clerks' offices.

General recommendations

Throughout the group's work, several general recommendations surfaced repeatedly. These recommendations are not linked to a single issue, but are relevant to all.

***Recommendations*:**

32. Determine recommendation priorities, action agents, and methods to achieve the recommendations.

33. Offer comprehensive training to clerks on management of electronic records systems; the four issues discussed in this report, for example, could form a part of the training.

34. Establish a mechanism to provide for the involvement of clerks in the development of state regulations and policies that have an impact on the recordkeeping responsibilities and practices of their offices, such as the appointment of liaisons between the associations and state agencies, or the development of an intergovernmental, interagency task force on records keeping.

Implementation

Implementation of the recommendations in this report cannot be discussed until the partners involved in their formulation review and accept the working group's findings (See Recommendation 32, above). The Office of the Secretary of the Commonwealth and the clerks' associations must jointly establish implementation priorities and methods. The working group members are committed to assisting in this process as necessary.

No action agents (parties responsible for carrying out each recommendation) have been assigned. This is an intentional omission; the Working Group believes that each recommendation should be examined individually and an appropriate partnership built for maximum flexibility and effectiveness.

Preservation

Introduction

Preservation is not a new concern; the need to preserve records of government actions extends to the earliest era of civilization, when the court scribes documented the stores of grain in the Mesopotamian warehouses. Then, as now, the goal of preservation has been to retain the informational content of the record, its structure (the unique format of the certificate, license, or correspondence), and its context (the identity of its authoring office or official and circumstances of its creation) for use, both in the present and over time. This once was as simple as preserving the physical media on which the information was stored, perhaps by filing the piece of paper alphabetically in a folder or filing cabinet. Not so anymore.

In order to preserve electronic records, we must preserve:

- √ the media on which the record is inscribed;
- √ the software with which the record was written;
- √ the hardware on which the software was run;
- √ the operating system controlling the hardware; and
- √ the documentation that shows users how to operate the hardware, use the software, and interpret the records.

At first, computer users thought that it would be necessary to start antique computer museums to house the old equipment when new computers were acquired; the next alternative considered was to set uniform standards so that all records could be preserved in a software- and hardware-independent form. Neither of these methods are possible, since the parts and software are unavailable for old computers and because data in new applications, like relational databases, are meaningless when separated from the software used to create them. Current preservation techniques emphasize *migration*, converting the data for use on the new computers.

But preservation is more than simply converting data. Hardware, software, and data documentation describes how and why the electronic records system created and used records and how the data is organized and encoded. Without documentation, preserved data will remain unintelligible and unusable.

Clerks are familiar with security measures for the protection of records from environmental hazards, vandalism, and disaster. Electronic records, too, require security; many of the protection techniques for electronic records are similar to those taken to protect textual records. In the case of disasters, however, electronic records may have to be removed from and used in a location outside town hall; with records dependent on hardware and software, how can the continuity of government be assured?

Technology standards: Before the technology revolution, records created by fountain pens, IBM electric typewriters, ballpoint pens, Remington manual typewriters, and pencils could all be read and understood because the information they contained and the manner of recording it was bounded by standards. Records shared the same alphabet and language, the same grammatical and structural conventions. These standards enabled textual information to be read, understood, shared, and transcribed meaningfully in other media-- regardless of how it was created.

Today, standards are equally as important. They permit electronic data to be exchanged among and read by different software and hardware products (see also, **Compatibility**, below). One model created to allow communication between different types of computers is called *Open Systems Interconnection* (OSI). By using the open systems model, data created and maintained on an existing computer system can be converted, or migrated, to new computer platforms because both generations of computers and software share the same basic conventions for operations, data management, and document construction. The risk of data loss is greatly reduced.

The Working Group believes that use of standards-based technology will support preservation goals.

***Recommendations*:**

1. Identify and publicize applicable hardware and software standards and operational practices that support forward migration of data to new platforms and software.

2. Develop a set of questions and requirements clerks can use in negotiating and contracting with vendors that will lead to the creation of non-proprietary, reliable, standards-based systems and records.

3. Establish a clearinghouse where clerks can report the success or failure of hardware, software, and media.

Preservation planning and migration: Even in standards-based systems, users must plan for the migration of data and the preservation of documentation that provides the structure and context of records. Planning questions include: what data will be converted? At what intervals? How will an audit trail documenting the conversion be created and what information will it include? What other information should be preserved?

These questions are critical to the long term accessibility and usefulness of records. For example, Working Group participants have concluded that *all* records that are retained in electronic format, both active and inactive, should be converted *every time* a system is upgraded. Technology doubles every eighteen months-- and with the average municipality upgrading or purchasing new systems every four years, there is no assurance of backwards compatibility across multiple generations of computers.

The Working Group believes that uniform preservation policies and procedures will be an advantage for clerks. Retention schedules are a part of these preservation policies and should offer clear guidelines for retention periods, office of record, and records media. Clerks seeking to retain the legality of electronic records over time can point to their compliance with the uniform standard as proof of good business practices.

Recommendations:

4. Review retention schedules to revise retention periods and identify the custodial office and media of the record copy.

5. Formulate uniform migration and preservation policies and procedures that support the preservation of all active and inactive records of long-term value, including security, backup, documentation, testing and migration methods and scheduling.

Security: All records, regardless of media, must be protected from environmental hazards, unauthorized access, mutilation, and loss. Electronic records, due to the fragility of magnetic media and the use of computer networks, are more vulnerable to loss than those in paper format. Special methods are required to secure electronic records. Security is vital to the use of records in the present, as well as the use of records over time.

Assessing the value of records can lead to informed and effective implementation of security measures. Electronic records used for tracking paper records or events, for example, will not require the same levels of protection as unique records having legal or long-term value. For these crucial electronic records systems and records, special measures are warranted, such as the identification of hardware and software at alternate sites that could be used in an emergency.

Recommendations:

6. To support disaster recovery efforts, coordinate and share information about the technology environment in each municipality with the goal of assisting municipalities to identify emergency data processing locations.

7. Formulate guidance on risk management analysis to assist clerks in assessing the level of security needed for various systems and records.

Compatibility

Introduction
Compatibility has importance in two arenas: communications and preservation. Prior to the advent of information technology, one merely had to be fluent in the written word to gain access to the document's message. Now communication via computer is limited by the ability of the hardware, software, and networks to interconnect to exchange information.

Compatibility is also a key concern in preservation, since records created with proprietary software and hardware may not be capable of being converted to new platforms. Open systems architecture supports both communication and data sharing, as well as migration activities to preserve electronic records.

The Open Systems Interconnection (OSI) model, developed by the International Standards Organization, is a set of specifications used as a basis for the construction of systems designed for the transfer of data. By using equipment that conforms or will conform to OSI, different manufacturers' machines can more effectively communicate and exchange data. Because OSI is an open, non-proprietary architecture, it can provide for consistency across generations of hardware and software, thus facilitating the preservation of and access to information of long-term value.

Compatibility, however, is often a secondary consideration in a free market society where the initial cost of the system drives decisions in fiscally-strapped communities; where volunteer computer study committees make long range decisions that impact communication capabilities for all municipal departments; and where the quixotic, constantly changing computer industry revises and upgrades information collection and storage on a weekly basis. In this environment, the best interests of the government can be supported by clerks who advocate for compatibility of records systems and methods; standardization of software; and coordination of data sharing and collection efforts.

Intra-office compatibility: Conversion of records from one software program to another, or major changes in hardware, presents a threat to data integrity and retention. For this reason, records custodians should emphasize compatibility when acquiring software for creation or migration of records.

In fact, within a clerk's office, there is often little uniformity in or compatibility among software packages. The Registry of Vital Records provides birth information on disk for any community that wants to participate in their program, but this software program may not be compatible with the clerk's system of storing business certificate information or U.C.C. filings, dog licensing records, census listings, or meeting minutes. It is quite common to have individual programs for each of these functions so that staff must be trained to use six or more software programs. The Central Voter Registry package adds a seventh program to this mix. This plethora of software applications reduces the productivity and efficiency of the office, prohibiting data sharing and requiring redundant data entry. In a perfect world, compatible programs would uniformly contain all data.

Clerks, as the creators and custodians of electronic records, can assist each other by identifying and promoting the use of effective, compatible, standards-based software applications.

Recommendations:

8. Offer an open session at association meetings to allow networking and discussion among municipal clerks regarding software application solutions to the problem of incompatibility within clerks' offices.

9. To promote compatibility, develop standards for functionality of software in an open systems environment.

Inter-office compatibility: We must encourage, endorse, and preserve the ability to interact with other municipal departments through interconnectable systems or networks. A community that allows an unobstructed flow of information between departments is able to function more efficiently. Such systems preclude the duplication of information gathering efforts and provide for the sharing of data among municipal departments.

Municipalities that introduce internal networks should use open architecture communication standards, such as the TCP/IP standard, to permit internal and external communication. Communities that use such standards can provide electronic access to residents through the Internet or dial-up connections.

The Working Group believes that inter-office compatibility can provide productivity and access benefits for all town offices.

Recommendations:

10. Advocate for municipality-wide, coordinated information technology acquisitions.

11. Promote the the development of compatible records systems within local governments.

External compatibility: The flow of critical information among municipalities and state agencies is hindered by incompatible systems at all levels. This obstacle may be partially overcome by the development of the Massachusetts Central Voter Registry.

When the Central Voter Registry was initially proposed, a survey of the 351 municipalities was conducted to determine which software program was most commonly used by Massachusetts communities. It quickly became obvious from this survey that the best route would be to design a program that would serve voter registry purposes, and provide each of the 351 municipalities with compatible equipment to operate the Voter Registration Information System (VRIS). This system, which includes a frequency random access device or a modem, a computer or computers, printers, and scanning wand for every city and town clerk's office in the state, will be in place by the end of

1995. At that time, every clerk will have compatible equipment and software that can interact not only with the Central Voter Registry, but with other communities as well. Electronic mail messaging is available through the VRIS network and when all communities are on-line, there is the possibility that other functions, such as business certificate registration, transmission of vital statistics information, and reporting to state agencies, will also be available. The network will permit state and local agencies to coordinate activities and disseminate state documents, proposed legislation, administrative regulations, and other information.

This ability to communicate with other government entities has the potential to revolutionize government activities; in order to reap the most benefit from this new tool, clerks must set their own course of action, rather than simply reacting to change.

Recommendations:

12. Explore the advisability of recommending that all on-line interaction between the municipalities and state agencies be conducted via the Voter Registration Information System (VRIS) network.

13. Form a joint association committee to coordinate efforts to share electronic data between the state agencies and the office of the municipal clerk.

Legality

Introduction
The ability to produce legally acceptable records in any format is critical to the functioning of the clerk's office. The legality of the records produced affects the day-to-day functioning of the municipality, the municipality's ability to enforce its rights and to bring and defend suit, and can have a profound effect on the citizens who rely on the office to provide them with reliable information and certificates.

Legal acceptance of public records flows from the processes by which such records are created, maintained, preserved and duplicated. These processes are designed to assure that the final product or record is accurate, trustworthy and reliable. Well-established standards and long-standing processes for the handling and care of non-electronic records provide these records with a high degree of validity and presumption of legality. Electronic systems, however, are subject to greater suspicion and scrutiny than their more traditional counterparts. This is due in part to their relative novelty and particularly to the ephemeral nature of the recording medium and the perception that they are more susceptible to alteration than are eye-readable records. If records created and maintained in electronic format are to become accepted as trustworthy in court and as a reliable means of conducting municipal business and documenting official information, there are a number of hurdles to be overcome.

Statutory authority: While case and statutory law do make provision for the use of electronic technologies, there continue to exist statutory obstacles to their acceptance. In some cases, these obstacles are embedded in statutes enacted long before computers were common and when magnetic or optical storage systems were envisioned. These statutes may require information or records to be "in writing" or to bear "a writing"; others may specify the means by which a record may be created and fail to include electronic systems. The latter case is ironic since, in many instances, these statutes were designed to embrace what were at the time new technologies, such as micrographics or xerographic processes, but have the ultimate effect of precluding the use of other, more modern systems.

The Working Group believes that these statutory obstacles to the creation and use of legally acceptable electronic records should be identified and removed. In revising these statutes, however, care should be exercised to ensure that the resulting records will be trustworthy and reliable.

Recommendations:

14. Identify statutes presenting obstacles to the acceptance of electronic recordkeeping systems and draft statutory language that will ensure the legality of a record based upon the circumstances of its creation and maintenance, regardless of the recording medium.

Creating a legally sufficient recordkeeping system: Even when there is no statutory impediment to the use of electronic recordkeeping systems, legal and cultural resistance to the acceptance of those records may be encountered. It is necessary for the users of the records to be confident of the validity and reliability of the information contained in the electronic systems, and for the systems themselves, along with their outputs, to be able to survive challenges to their trustworthiness in court. The major difference between paper and computer records lies in the laying of a proper foundation prior to introduction into evidence. Thus, the conditions surrounding the creation and maintenance of electronic records will profoundly affect whether they are to be admissible in evidence. In its discussions, the Working Group identified a number of factors which it felt to be critical to both the reliability of the records and the consequent confidence of the user:

√ the source and structure of the record must be known to be authentic;
√ the authenticity of the record must be preserved;
√ the record must be created according to law;
√ standard procedures must be followed in the creation, use, and reproduction of the record;
√ the system producing the record must be used in the routine operation of the office;
√ the system used to produce the record must be shown to be reliable;
√ quality control procedures must be put in place to ensure the accuracy of the record;
√ there must be a legal mandate for the acceptance of the electronic record;
√ there must be a process for the verification and unique identification of each record;
√ audit trails must be maintained to document the integrity of the content of the record and to document all access to the data; and
√ external, neutral third-party audit control must be maintained to ensure the integrity of the system.

These requirements will also ensure that the recordkeeping system is functional over time and produces reliable and operationally useful outputs as required. Much work has been done in this area in other jurisdictions; federal statutes such as the Uniform Preservation of Private Business Act, the Uniform Records Retention Act, the Uniform Photographic Copies of Business and Public Record as Evidence Act, the Federal Rules of Evidence, and state guidelines, such as the State of New York's "Guidelines for the Legal Acceptance of Public Records in an Emerging Electronic Environment", provide some guidance. Building upon these and other state and Federal statutes and guidelines, regulations or guidelines should be drafted to ensure the creation of legally acceptable records.

Recommendations:

15. Clarify the terms *original* and *copy* as they relate to electronic records.

16. Formulate guidance on the attestation and certification of electronic records.

17. Formulate a uniform set of recordkeeping policies and good practices that can be widely adopted and promoted.

18. Establish clearly defined standards for the creation and maintenance of records that are trustworthy, reliable and legal.

19. Investigate the viability of models for achieving recordkeeping standards, either through a central registry system or by having a single entity set performance standards or regulations for recordkeeping systems.

Security and preservation of the legal record: Regardless of physical format, records must be maintained over periods of time. As with traditional paper and film records having legal value, custodians must provide for the physical and intellectual security of their electronic records. Records need to be protected from environmental damage, loss and mischief. Records need to be stored in circumstances which prevent the loss of data from disaster or environmental degradation, and must be properly identified so that the data contained in them can be readily accessed and used.

Records must be periodically recopied as the storage medium ages. Precautions must be taken to ensure that the information is not tampered with through implementation of physical security measures and other controls such as audit trails indicating all occasions on which the records were accessed or manipulated.

The Working Group believes that the ability to maintain the legal value of the record over time is critical. With municipalities upgrading their systems on an average of every 44 months, electronically-stored data will frequently need to be migrated forward to new platforms. Records custodians will need to be able to demonstrate how the conversion was done and that it was done properly, with no loss of data. The courts have not yet looked at forward migration of records and it may be necessary to show the court how the "original" looked.

Recommendations:

20. Set standards for the storage, duplication, back up or dispersal of records, and for their proper identification.

21. Establish standards for the use of audit trails to ensure the intellectual security of records.

22. Determine expected longevity of various media and establish guidelines for the periodic recopying of records.

23. Establish standards and time frames for migrating records forward to new operating systems and platforms.

24. Investigate the desirability of alternative storage media for records with long-term value, such as microfilm.

Access

Introduction
Government records are a by-product of government actions and thus are a direct link to accountability. Records are critical to the achievement of government objectives and the communication of its intentions and actions to the governed. Records also document our society, who we are as a community and as individuals. Because they have value for many purposes-- administrative, legal, fiscal, sociological, personal, historical, scientific-- some government records are retained permanently. Preservation of such records is pointless if records are not accessible to the government and the public.

Perhaps because they are so valuable, access to government records is a controversial issue. Even within interest groups, persons have conflicting views and strong opinions on public access, privacy rights, resale of government information, and potential misuse of records. With the development of transactional electronic records systems and the reality of paperless systems not too far in the future, this debate is growing in volume and importance. In the midst of this environment, there is a need for more guidance and uniform standards that clerks can adopt to ensure reasonable and fair access practices.

Electronic access and the law: Despite the fact that the public records laws were established before the development of computers, the law has been interpreted on a case by case basis to satisfy most creators and requesters of electronic government records. Until recently, many electronic records systems were used for tracking or indexing of paper records, or for processing of text that would be printed out on paper. New types of systems, networks, and uses for electronic records present additional challenges to the appropriate provision of access and require further analysis.

There may be no paper equivalent for some electronic records. An automated database may contain information that would once have been created and maintained as different records; in fact, these traditional types of records may still be generated as reports output from the database. But what happens when a requester wishes to directly query the database, combining information from different reports? As electronic records systems become more sophisticated, this type of request will occur with greater frequency. The Working Group believes that the public has an interest in access to government information and in personal privacy. The public also has an interest in maintaining the integrity of records by protecting them from alteration and in the efficiency of government operations. For this reason, the group sees the need for guidance relating to the provision of access to on-line information.

There are other aspects of access to electronic records that require analysis and development of guidance. For example, electronic records systems often contain both information that is restricted and information that is public. Unlike paper records, the ability to segregate data must be established before records are created, when the system is designed. What is the custodian's responsibility to provide for segregation?

Another important access issue is the question of fees. In the case of paper records, the cost of obtaining information is closely related to the cost of providing access to and copies of records. For example, the cost of completing a license form is relatively low, as is the cost of providing a copy of the record. In contrast, electronic records can be costly to obtain. Does this differential argue for sliding scale or fee system that could return revenue to the community? In such a system, could the potential use influence fees? An appeal to a third party, a public records commission, for example, might help to provide an assurance of fairness.

The advent of electronic records also gives rise to confusion about the term *custodian*.. Electronic records may be in the physical custody of the data processing department: in this case,who is the custodian-- the data processing director or the clerk? Who has responsibility to provide access or certify copies? As described in G. L. c. 66, a major custodial responsibility is preservation of records; who is responsible for making sure that electronic records are properly migrated to new platforms or recopied as needed? This is not a trivial issue since it is possible that considerable costs could be involved-- and considerable liability if preservation actions fail to be taken. Some clerks employ vendors to maintain electronic records; in these cases, is the vendor a legal custodian, bound by public records law?

***Recommendations*:**

25. Develop uniform guidance on access to electronic records, considering specifically:
    - direct public access to on-line data;
    - methods to protect on-line data from unauthorized public access and alteration;
    - the impact of direct public access to on-line data on the efficiency of government operations;
    - subscription and licensing arrangements for on-line data;
    - records custodian responsibility to provide for segregation in systems design; and
    - the public records status of licensed software packages.

26. Investigate the application of the public records law to commercial requests for access to and copies of electronic records.

27. Develop uniform guidance on fees for copies of electronic records.

28. Clarify the term *records custodian* as it applies to electronic records that may exist in more than one location; and the responsibilities of the custodian for access, copying, certification, and preservation.

Privacy issues: Disclosure of information about residents is a long-term concern of municipal clerks. This concern is not peculiar to electronic records since the same information is available in paper format as well. What electronic records systems introduce to this issue, however, is the ability of requesters to acquire different types of records that can be quickly and easily manipulated and linked to reveal a clearer picture of individuals than previously available. The potential for commercial exploitation of this linkage may lead to a situation where citizens question the validity of government data collection for any purpose.

The Working Group believes that two critical activities should be initiated: assessment of the need for data collection and review of current restrictions. Limiting data collection is not a new idea. G. L. c. 66A addresses this question and requires state agencies to limit the personal data collected to only that needed to accomplish agency business and to destroy such data when it is no longer relevant to agency goals. Moreover, examining information collection in the light of business needs is simply a good management practice; considerable costs are attached to data collection and storage.

It may also be necessary to review the current restrictions on personal data. This review should focus on the question of what is reasonable access. There may be laws that provide insufficient protection as well as those that are too restrictive. An example of the latter is the case of out-of-wedlock births; illegitimacy is no longer a social stigma. Should the law reflect this change in attitude?

***Recommendations*:**

29. In the context of electronic records systems' ability to manipulate and link data, review data collection requirements and privacy restrictions.

Indexing for access: Unlike paper-based records, electronic records are inaccessible without a proper index. Unindexed, paper records can still be used, but an optical disk without an index is simply a frisbee. Since it is so labor-intensive to correct poorly indexed electronic records-- where it is possible to make corrections at all-- it is vital to plan for indexing before creating records. Index construction should be part of systems procurement contracts. Software packages should include superior ability to index records.

Uniform indexing rules could enhance clerks' ability to ensure the accessibility and efficiency of their records systems over time, as well as provide some compatibility for clerks and their publics across municipalities.

***Recommendations*:**

30. Develop uniform guidance for specifying and analyzing index generators included in application software.

31. Establish standard indexing and filing rules for use by clerks' offices.

APPENDIX A: Working Group Members and Guests

Karen Anderson, City Clerk
City of Malden

Kathryn Hammond Baker, Assistant Archivist for
Records Management and Acquisitions
Massachusetts Archives

David Best, Public Records Analyst
Massachusetts Archives

Joyce Bradshaw, Town Clerk
Town of North Andover

Robert Brennan, Director of Management Information Systems
City of Quincy

Shauna Cully, Associate Counsel
Division of Public Records

Shirley S. Davenport, Town Clerk
Town of Sharon

Saran Gillies, Town Clerk
Town of Braintree

John Hanlon, City Clerk
City of Everett

Peter Koutoujian, City Clerk
City of Waltham

Kelly MacWilliam, Associate Counsel
Division of Public Records

Natalie Maga, City Clerk
City of Peabody

Constance E. Perron, City Clerk
City of Beverly

Patrick J. Ward, Town Clerk
Town of Brookline

Richard Walsh, Director of Management Information Systems
City of Newton

APPENDIX B: List of Recommendations

Preservation:

1. Identify and publicize applicable hardware and software standards and operational practices that support forward migration of data to new platforms and software.
2. Develop a set of questions and requirements clerks can use in negotiating and contracting with vendors that will lead to the creation of non-proprietary, reliable, standards-based systems and records.
3. Establish a clearinghouse where clerks can report the success or failure of hardware, software, and media.
4. Review retention schedules to revise retention periods and identify the custodial office and media of the record copy.
5. Formulate uniform migration and preservation policies and procedures that support the preservation of all active and inactive records of long-term value, including security, backup, documentation, testing and migration methods and scheduling.
6. To support disaster recovery efforts, coordinate and share information about the technology environment in each municipality with the goal of assisting municipalities to identify emergency data processing locations.
7. Formulate guidance on risk management analysis to assist clerks in assessing the level of security needed for various systems and records.

Compatibility:

8. Offer an open session at association meetings to allow networking and discussion among municipal clerks regarding software application solutions to the problem of incompatibility within clerks' offices.
9. To promote compatibility, develop standards for functionality of software in an open systems environment.
10. Advocate for municipality-wide, coordinated information technology acquisitions.
11. Promote the the development of compatible records systems within local governments.
12. Explore the advisability of recommending that all on-line interaction between the municipalities and state agencies be conducted via the Voter Registration Information System (VRIS) network.

13. Form a joint association committee to coordinate efforts to share electronic data between the state agencies and the office of the municipal clerk.

Legality:

14. Identify statutes presenting obstacles to the acceptance of electronic recordkeeping systems and draft statutory language that will ensure the legality of a record based upon the circumstances of its creation and maintenance, regardless of the recording medium.

15. Clarify the terms *original* and *copy* as they relate to electronic records.

16. Formulate guidance on the attestation and certification of electronic records.

17. Formulate a uniform set of recordkeeping policies and good practices that can be widely adopted and promoted.

18. Establish clearly defined standards for the creation and maintenance of records that are trustworthy, reliable and legal.

19. Investigate the viability of models for achieving recordkeeping standards, either through a central registry system or by having a single entity set performance standards or regulations for recordkeeping systems.

20. Set standards for the storage, duplication, back up or dispersal of records, and for their proper identification.

21. Establish standards for the use of audit trails to ensure the intellectual security of records.

22. Determine expected longevity of various media and establish guidelines for the periodic recopying of records.

23. Establish standards and time frames for migrating records forward to new operating systems and platforms.

24. Investigate the desirability of alternative storage media for records with long-term value, such as microfilm.

Access:

25. Develop uniform guidance on access to electronic records, considering specifically:
    - direct public access to on-line data;
    - methods to protect on-line data from unauthorized public access and alteration;
    - the impact of direct public access to on-line data on the efficiency of government operations;
    - subscription and licensing arrangements for on-line data;
    - the records custodian's responsibility to provide for segregation in systems design; and
    - the public records status of licensed software packages.

26. Investigate the application of the public records law to commercial requests for access to and copies of electronic records.

27. Develop uniform guidance on fees for copies of electronic records.

28. Clarify the term *records custodian* as it applies to electronic records that may exist in more than one location; and the responsibilities of the custodian for access, copying, certification, and preservation.

29. In the context of electronic records systems' ability to manipulate and link data, review data collection requirements and privacy restrictions.

30. Develop uniform guidance for specifying and analyzing index generators included in application software.

31. Establish standard indexing and filing rules for use by clerks' offices.

General Recommendations:

32. Determine recommendation priorities, action agents, and methods to achieve the recommendations.

33. Offer comprehensive training to clerks on management of electronic records systems; the four issues discussed in this report, for example, could form a part of the training.

34. Establish a mechanism to provide for the involvement of clerks in the development of state regulations and policies that have an impact on the recordkeeping responsibilities and practices of their offices, such as the appointment of liaisons between the associations and state agencies, or the development of an intergovernmental, interagency task force on records keeping.

APPENDIX C: List of Readings

READINGS

ERWG members were provided with readings from a variety of sources including:

American National Standards Institute Technical Report. "Technical Report for Information and Image Management - Performance Guidelines for the Legal Acceptance of Records Produced by Information Technology Systems; Part III: Implementation of the Performance Guideline for the Legal Acceptance of Records Produced by Information Technology Systems. - ANSI/AIIM TR-31-1994." Silver Spring: Association of Information and Image Management, 1994.

American National Standards Institute Technical Report. "Technical Report for Information and Image Management - Performance Guidelines for the Legal Acceptance of Records Produced by Information Technology Systems; Part I: Performance Guideline for Admissibility of Records Produced by Information Technology Systems as Evidence. - ANSI/AIIM TR-31-1992." Silver Spring: Association of Information and Image Management, 1992.

Attinger, Monique. "Integrated Information Management: A Real World Theory." Association of Records Managers and Administrators, *Proceedings of the 39th Annual Conference,* Toronto, 1994.

Cook, Terry. "It's 10 O'Clock: Do You Know Where Your Data Are?" *Technology Review*, January 1995.

Elliott, A. R. "Fundamentals of Managing On-Line and Networked Records." Association of Records Managers and Administrators, *Proceedings of the 39th Annual Conference*, Toronto, 1994.

Rothenberg, Jeff. "Ensuring the Longevity of Digital Documents." *Scientific American*, January 1995.

Wright, Ellen. "Incriminating Data." *Hemispheres*, 1995.

Several articles were also excerpted from *Government Technology.*

Referenced government guidelines, rules and regulations include:

State of Florida. Rules of the Department of State. Division of Library and Information Services. “Chapter 1B-26.003 Electronic Recordkeeping.”

Commonwealth of Massachusetts. Office of the Secretary of the Commonwealth. Kelly MacWilliam, Memorandum, "Data Compilations." May, 1995.

State of New Mexico. New Mexico Commission for Public Records. SRC Rule 93-05. "Performance Guidelines for the Legal Acceptance of Public Records Produced by Information Technology Systems." 1993.

State of New York. State Archives and Records Administration. “Guidelines for the Legal Acceptance of Public Records in an Emerging Electronic Environment.” 1994.

Commonwealth of Pennsylvania. Governor's Office. Management Directive, "Electronic Records Management." 1994.

State of Texas. Texas State Library, State and Local Records Management Division. Local Government Bulletin Number Two: "Electronic Record Standards and Procedures." 1993.

United States Department of Justice. Justice Management Division, Systems Policy Staff. "Admissibility of Electronically Filed Federal Records as Evidence." October, 1990.

Commonwealth of Virginia. The Library of Virginia. "Guidelines for Managing Electronic Records."